



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/791,297	03/01/2004	Silvano Gai	ANDIP024A	3525
22434	7590	09/10/2007	EXAMINER	
BEYER WEAVER LLP			MILLS, DONALD L	
P.O. BOX 70250			ART UNIT	PAPER NUMBER
OAKLAND, CA 94612-0250			2616	
MAIL DATE		DELIVERY MODE		
09/10/2007		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	Application No.	Applicant(s)
	10/791,297	GAI ET AL.
	Examiner Donald L. Mills	Art Unit 2616

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 01 March 2004.
- 2a) This action is FINAL.                    2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-42 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1-42 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 20 September 2004 is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All    b) Some \* c) None of:
  1. Certified copies of the priority documents have been received.
  2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | Paper No(s)/Mail Date. _____                                      |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>06/07/2004; 11/22/2004</u> | 5) <input type="checkbox"/> Notice of Informal Patent Application |
|   | 6) <input type="checkbox"/> Other: _____                          |

**DETAILED ACTION*****Claim Rejections - 35 USC § 102***

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1, 2, 4, and 5 are rejected under 35 U.S.C. 102(e) as being anticipated by Walker et al. (US 2002/0163920 A1), hereinafter referred to as Walker.

Regarding claim 1, Walker discloses a method and apparatus for providing network security, which comprises:

*Receiving a packet (Referring to Figure 1, packets for routing are received. See paragraph 0039;)*

*Classifying the packet as having a security group designation selected from a plurality of security group designations, the security group designation associating a set of destinations and a set of sources authorized to access the set of destinations (Referring to Figure 1, packet destined to be routed over different VLANs have different security associations, the security association authorizes routing or switching from specific sources to specific destinations via tunnels. See paragraphs 0035, 0039, and 0044; and*

*Applying a security group tag to the packet which identifies the security group designation, the security group tag being applied in a field not reserved for virtual local area*

*network information* (Referring to Figure 1, during the preparation process authentication information is added to each payload packet, which is not in a designated VLAN field. See paragraph 0014.)

Regarding claims 2 and 5, Walker discloses *wherein the security group tag is applied in a field reserved for layer one* (Referring to Figure 1, during the preparation process authentication information is added to each payload packet, at the physical layer since it is not included in the Layer-2 or Layer-3 header. See paragraph 0014.)

Regarding claim 4, Walker discloses a method and apparatus for providing network security, which comprises:

*Receiving a packet* (Referring to Figure 1, packets for routing are received. See paragraph 0039;)

*Classifying the packet as having a security group designation selected from a plurality of security group designations, the security group designation associating a set of destinations and a set of sources authorized to access the set of destinations* (Referring to Figure 1, packet destined to be routed over different VLANs have different security associations, the security association authorizes routing or switching from specific sources to specific destinations via tunnels. See paragraphs 0035, 0039, and 0044;) and

*Applying a security group tag to the packet which identifies the security group designation, the security group tag being applied in a field reserved for security group information* (Referring to Figure 1, during the preparation process authentication information is added to each payload packet, thereby considered reserved since the intended placement of the authentication information relates to the payload packet. See paragraph 0014.)

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 3 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Walker (US 2002/0163920 A1) in view of Heggarty et al. (US 2003/0235191 A1), hereinafter referred to as Heggarty.

Regarding claims 3 and 6 as explained in the rejection statement of claims 1 and 4, Walker discloses all of the claim limitations of claims 1 and 4 (parent claims).

Walker does not disclose *wherein the security group tag is applied in a field reserved for layer two.*

Heggarty teaches utilizing the VLAN ID from the Q-tag in the Ethernet frame header (layer-2) for packet forwarding in a switch (See paragraph 0048.)

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement the Layer-2 tagging of Heggarty in the system of Walker. One of ordinary skill in the art at the time of the invention would have been motivated to do so in order to improve system efficiency and reduce system processing by implementing the authentication information in the VLAN Ethernet header for Layer-2 networks as taught by Walker (See paragraphs 0009 and 0014.)

Art Unit: 2616

5. Claims 7-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Walker (US 2002/0163920 A1) in view of Van Seters et al. (US 5,978,378), hereinafter referred to as Van Seters.

Regarding claims 7, 14, 18-21, 29-32, and 38, Walker discloses a method and apparatus for providing network security, which comprises:

*Receiving a packet* (Referring to Figure 1, packets, comprising a first and subsequent packets, for routing are received. See paragraph 0039;)

*Classifying the packet as having a security group designation selected from a plurality of security group designations, wherein the first security group designation associating a first set of destinations and a first set of sources authorized to access the first set of destinations* (Referring to Figure 1, packets, comprising a first and subsequent packets, destined to be routed over different VLANs have different security associations, the security association authorizes routing or switching from specific sources to specific destinations via tunnels. See paragraphs 0035, 0039, and 0044;) and

*Applying a security group tag to the packet which identifies the first security group designation* (Referring to Figure 1, during the preparation process authentication information is added to each payload packet, first and subsequent packet, which is not in a designated VLAN field and utilized to verify the authenticity of the packet. See paragraph 0014.)

Walker does not disclose *wherein the security group tag being applied in a field reserved for layer three or higher and wherein the information in the field is not used in forwarding decisions by interswitch links.*

Walker teaches during the preparation process authentication information is added to each payload packet, at the physical layer since it is not included in the Layer-2 or Layer-3 header (See paragraph 0014.) However, Van Seters teaches identifying VLAN members by a field located at the layer-3 header of each data unit (See column 1, lines 28-30 and 35-62.)

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement the authentication information of Walker in the Layer-3 header of Van Seters. One of ordinary skill in the art at the time of the invention would have been motivated to do so in order to improve system efficiency and reduce system processing by implementing the authentication information in the VLAN IP header for Layer-3 networks as taught by Walker (See paragraphs 0009 and 0014.)

Regarding claims 8, 22, and 23, the primary reference further teaches *providing authentication information in the first packet* (Referring to Figure 1, during the preparation process authentication information is added to each payload packet, which is not in a designated VLAN field, for authentication purposes. See paragraph 0014.)

Regarding claims 9 and 24, the primary reference further teaches *encrypting/decrypting the first security group tag* (Referring to Figure 1, the packet is encrypted and decrypted. See paragraph 0036.)

Regarding claims 10 and 27, the primary reference further teaches:  
*Receiving a second packet* (Referring to Figure 1, packets, comprising a first and second packet, for routing are received. See paragraph 0039;)

*Classifying the second packet as having a security group designation selected from a plurality of security group designations, wherein the second security group designation*

*associating a first set of destinations and a first set of sources authorized to access the first set of destinations* (Referring to Figure 1, each first and subsequent packet destined to be routed over different VLANs have different security associations, the security association authorizes routing or switching from specific sources to specific destinations via tunnels. See paragraphs 0035, 0039, and 0044; ) and

*Applying a security group tag to the packet which identifies the second security group designation* (Referring to Figure 1, during the preparation process authentication information is added to each first and subsequent payload packet, which is not in a designated VLAN field. See paragraph 0014.)

Regarding claim 11, the primary reference further teaches *receiving the packet directly from a source node* (Referring to Figure 1, the tunnel is established between a source and destination. See paragraph 0038.)

Regarding claim 12, the primary reference further teaches *classifying the packet based on a source identity* (Referring to Figure 1, the tunnel is established between a source and destination, in which the preparation process adds authentication information to the packet in accordance with the source creating the tunnel. See paragraph 0014 and 0038.)

Regarding claim 13, the primary reference further teaches *classifying the packet based on a payload content* (Referring to Figure 1, the tunnel is established between a source and destination, in which the preparation process adds authentication information to the packet in accordance with the source creating the tunnel and packet payload. See paragraph 0014 and 0038.)

Regarding claim 15, the primary reference further teaches *wherein the second set of sources comprise a source that is included in the first set of sources* (Referring to Figure 1, the tunnel is established between a source and destination, in which the preparation process adds authentication information to the packet in accordance with the source creating the tunnel and packet payload. See paragraph 0014 and 0038.)

Regarding claim 16, the primary reference further teaches *wherein the second set of destinations comprise a destination that is included in the first set of destinations* (Referring to Figure 1, the tunnel is established between a source and destination, in which the preparation process adds authentication information to the packet in accordance with the source creating the tunnel and packet payload. See paragraph 0014 and 0038.)

Regarding claim 25, the primary reference further teaches *wherein the first security group is a closed group* (Referring to Figure 1, the tunnel is established between a source and destination, in which the preparation process adds authentication information to the packet in accordance with the source creating the tunnel (closed group) and packet payload. See paragraph 0014 and 0038.)

Regarding claim 26, the primary reference further teaches *wherein the first security group is a partially overlapping group* (Referring to Figure 1, the tunnel is established between a source and destination, in which the preparation process adds authentication information to the packet in accordance with the source creating the tunnel and packet payload which spans nodes (partially overlapping group). See paragraph 0014 and 0038.)

Regarding claims 28, 34, 36, and 40, the primary reference further teaches *applying a policy to the packet based upon the first security group and the destination address, wherein the*

*policy is selected from the group of actions consisting of: forwarding the packet; forwarding the packet and making a record of forwarding the packet; dropping the packet; dropping the packet and making a record of the dropping the packet; and inspecting other fields of the packet to determine how to dispose of the packet (Referring to Figure 1, the security association of the packet specifies the routing of the packet and whether the packet is forwarded or discarded. See paragraph 0039.)*

Regarding claims 33 and 39, the primary reference further teaches *wherein the method is implemented on a router* (Referring to Figure 1, the direct routing method is implemented on a layer 3 device. See paragraph 0037.)

Regarding claims 35 and 41, the primary reference further teaches *wherein the router resides in a local area network of a multi-LAN enterprise network and physically connects, directly, to a host* (Referring to Figure 1, the layer 3 device resides in a LAN of multi LAN network and physically connects the source and destination.)

Regarding claims 37 and 42, the primary reference further teaches *wherein transmitting the packet or denying transmission or delaying transmission of the packet effects the level of service constraint, and wherein different security groups correspond to different levels of service* (Referring to Figure 1, the system comprises authentication logic, decision logic and routing logic based on security associations. See paragraph 0028.)

### ***Conclusion***

Art Unit: 2616

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Donald L. Mills whose telephone number is 571-272-3094. The examiner can normally be reached on 8:00 AM to 4:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chi Pham can be reached on 571-272-3179. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Donald L Mills/

August 31, 2007

  
CHI PHAM  
SUPERVISORY PATENT EXAMINER  
9/4/07